CLAIMS

What is claimed is:

1. A method comprising:

receiving a request from a client; and

pre-authorizing the client, in response to the request, to allow actions by a user as a member of a group of users by sending to the client offline access information comprising a first key associated with the group, the first key being useable at the client to access an electronic document by decrypting a second key in the electronic document.

2. The method of claim 1, wherein pre-authorizing the client comprises comparing a time of last recorded client-synchronization with a time of last change in user-group information for the user.

3. The method of claim 1, wherein pre-authorizing the client comprises comparing current user-group information for the user with received user-group information for the user from the client.

4. The method of claim 1, wherein the client allows actions with respect to the electronic document based on document-permissions information residing in the electronic document.

5. The method of claim 1, wherein the offline access information further comprises document-permissions information associated with multiple documents, including the electronic document, and the client allows actions with respect to the electronic document based on the document-permissions information.

6. The method of claim 1, wherein receiving a request comprises receiving a request from the client to take an action with respect to a second document.

7. The method of claim 6, further comprising verifying the user at the client as an authenticated user.

8. The method of claim 6, wherein the offline access information further comprises:

at least one user-specific key;

at least one group-specific key, including the first key; and

at least one set of document-permissions information associated with multiple documents.

9. The method of claim 8, further comprising receiving an offline audit log from the client.

10. The method of claim 8, wherein the at least one set of document-permissions information comprises one or more policies associated with the second document, and the offline access information further comprises a document revocation list.

11. The method of claim 8, wherein the offline access information further comprises at least one set of document-permissions information associated with a specific document selected based on synchronization prioritization information.

12. A method comprising:

receiving from a document control server, when online, offline access information comprising a first key associated with a group of users of the document control server; and

allowing access to an electronic document, when offline, by performing operations comprising using the first key to decrypt a second key in the electronic document and governing actions with respect to the electronic document based on document-permissions information associated with the electronic document.

13. The method of claim 12, wherein governing actions with respect to the electronic document comprises obtaining the document-permissions information from the electronic document.

14. The method of claim 12, wherein governing actions with respect to the electronic document comprises:

identifying a document policy reference in the electronic document; and

obtaining locally retained document-permissions information based on the document policy reference.

15. The method of claim 12, wherein the offline access information comprises at least one user-specific key, at least one group-specific key, including the first key, at least one set of document-permissions information associated with multiple documents, and a document revocation list.

16. The method of claim 12, further comprising preventing access to the document, when offline, if a difference between a current time and a receipt time of the offline access information exceeds a server-synchronization-frequency parameter.

17. The method of claim 16, wherein the server-synchronization-frequency parameter is specific to the document.

18. The method of claim 12, further comprising:

maintaining an offline audit log; and

uploading the offline audit log when online.

19. A method comprising:

encrypting an electronic document; and

incorporating into the encrypted electronic document an address of a document control server, document-permissions information, and an encryption key useable in decrypting the encrypted electronic document, the encryption key being encrypted with a key generated by, and associated with a group of users of, the document control server.

20. The method of claim 19, wherein the encryption key comprises a session key generated by the document control server, encrypting the electronic document comprises encrypting the electronic document using a document key, and incorporating comprises incorporating into the encrypted electronic document a document security payload comprising the document key and the document-permissions information, the document security payload being encrypted using the session key.

21. The method of claim 20, wherein the document security payload further comprises a document identifier assigned by the document control server, and incorporating further comprises incorporating into the encrypted electronic document a copy of the session key encrypted using a public key associated with the document control server.

22. The method of claim 19, wherein the document-permissions information specifies access permissions at a level of granularity smaller than the electronic document.

23. A software product tangibly embodied in a machine-readable medium, the software product comprising instructions operable to cause one or more data processing apparatus to perform operations comprising:

receiving a request from a client; and

pre-authorizing the client, in response to the request, to allow actions by a user as a member of a group of users by sending to the client offline access information comprising a first key associated with the group, the first key being useable at the client to access an electronic document by decrypting a second key in the electronic document.

24. The software product of claim 23, wherein pre-authorizing the client comprises comparing a time of last recorded client-synchronization with a time of last change in user-group information for the user.

25. The software product of claim 23, wherein pre-authorizing the client comprises comparing current user-group information for the user with received user-group information for the user from the client.

26. The software product of claim 23, wherein the client allows actions with respect to the electronic document based on document-permissions information residing in the electronic document.

27. The software product of claim 23, wherein the offline access information further comprises document-permissions information associated with multiple documents, including the electronic document, and the client allows actions with respect to the electronic document based on the document-permissions information.

28. The software product of claim 23, wherein receiving a request comprises receiving a request from the client to take an action with respect to a second document.

29. The software product of claim 28, wherein the operations further comprise verifying the user at the client as an authenticated user.

30. The software product of claim 28, wherein the offline access information further comprises:

at least one user-specific key;
at least one group-specific key, including the first key; and
at least one set of document-permissions information associated with multiple documents.

31. The software product of claim 30, wherein the operations further comprise receiving an offline audit log from the client.

32. The software product of claim 30, wherein the at least one set of document-permissions information comprises one or more policies associated with the second document, and the offline access information further comprises a document revocation list.

33. The software product of claim 30, wherein the offline access information further comprises at least one set of document-permissions information associated with a specific document, and the operations further comprise selecting the document-specific document-permissions information based on synchronization prioritization information.

34. A software product tangibly embodied in a machine-readable medium, the software product comprising instructions operable to cause one or more data processing apparatus to perform operations comprising:

receiving from a document control server, when online, offline access information comprising a first key associated with a group of users of the document control server; and

allowing access to an electronic document, when offline, by performing operations comprising using the first key to decrypt a second key in the electronic document and governing actions with respect to the electronic document based on document-permissions information associated with the electronic document.

35. The software product of claim 34, wherein governing actions with respect to the electronic document comprises obtaining the document-permissions information from the electronic document.

36. The software product of claim 34, wherein governing actions with respect to the electronic document comprises:

identifying a document policy reference in the electronic document; and

obtaining locally retained document-permissions information based on the document policy reference.

37. The software product of claim 34, wherein the offline access information comprises at least one user-specific key, at least one group-specific key, including the first key, at least one set of document-permissions information associated with multiple documents, and a document revocation list.

38. The software product of claim 34, wherein the operations further comprise preventing access to the document, when offline, if a difference between a current time and a receipt time of the offline access information exceeds a server-synchronization-frequency parameter.

39. The software product of claim 38, wherein the server-synchronization-frequency parameter is specific to the document.

40. The software product of claim 34, wherein the operations further comprise:

maintaining an offline audit log; and

uploading the offline audit log when online.

41. A software product tangibly embodied in a machine-readable medium, the software product comprising instructions operable to cause one or more data processing apparatus to perform operations comprising:

encrypting an electronic document; and

incorporating into the encrypted electronic document an address of a document control server, document-permissions information, and an encryption key useable in decrypting the encrypted electronic document, the encryption key being encrypted with a key generated by, and associated with a group of users of, the document control server.

42. The software product of claim 41, wherein the encryption key comprises a session key generated by the document control server, encrypting the electronic document comprises encrypting the electronic document using a document key, and incorporating comprises incorporating into the encrypted electronic document a document security payload comprising the document key and the document-permissions information, the document security payload being encrypted using the session key.

43. The software product of claim 42, wherein the document security payload further comprises a document identifier assigned by the document control server, and incorporating further comprises incorporating into the encrypted electronic document a copy of the session key encrypted using a public key associated with the document control server.

44. The software product of claim 41, wherein the document-permissions information specifies access permissions at a level of granularity smaller than the electronic document.

45. A system comprising:

a document control server that synchronizes offline access information with a client in response to a client request, the offline access information comprising a first key associated with a group, the first key being useable at the client to access an electronic document by decrypting a second key in the electronic document; and

the client that allows access to the electronic document, when offline, by a user as a member of the group, using the first key to decrypt the second key in the electronic document and governing actions with respect to the electronic document based on document-permissions information associated with the electronic document.

46. The system of claim 45, wherein the electronic document comprises the document-permissions information.

47. The system of claim 46, wherein the second key comprises a session key generated by the document control server, and the electronic document further comprises a document security payload comprising a document key and the document-permissions information, the document security payload being encrypted using the session key.

48. The system of claim 45, wherein the offline access information further comprises:

at least one user-specific key;

at least one group-specific key, including the first key; and

at least one set of document-permissions information associated with multiple documents.

49. The system of claim 45, wherein the client comprises an agent that periodically contacts the document control server to synchronize the offline access information.

50. The system of claim 45, wherein the document control server comprises:

a server core with configuration and logging components;

an internal services component that provides functionality across dynamically loaded methods; and

dynamically loaded external service providers, including one or more access control service providers.

51. The system of claim 45, further comprising:

a business logic tier comprising a cluster of document control servers, including the document control server;

an application tier including the client comprising a viewer client, a securing client, and an administration client; and

a load balancer that routes client requests to the document control servers.

52. The system of claim 45, wherein the client request comprises a request from the client to take an action with respect to a second document.

53. The system of claim 52, wherein the document control server comprises a permissions-broker server including a translation component, the second document comprises a document secured previously by the permissions-broker server, and the translation component being operable to translate first document-permissions information in a first permissions-definition format into second document-permissions information in a second permissions-definition format in response to the request being received from the client.

54. The system of claim 52, wherein the server comprises a permissions-broker server operable to identify information associated with the second document in response to the request, the associated information being retained at the server and indicating a third electronic document different from and associated with the second document, the server being operable to relate information concerning the third electronic document to the client to facilitate the action to be taken.

55. The system of claim 52, wherein the server comprises a permissions-broker server operable to obtain and send, in response to the request, a software program comprising instructions operable to cause one or more data processing apparatus to perform operations effecting an authentication procedure, and the client uses the authentication program to identify a current user and control the action with respect to the second document based on the current user and document-permissions information associated with the second document.

56. A system comprising:

server means for transparently providing offline access information for controlled documents to pre-authorize a client to allow actions by a user as a member of a group of users, the offline access information comprising a first key associated with the group, the first key being useable at the client to access an electronic document by decrypting a second key in the electronic document; and

client means for accessing the electronic document using the offline access information.

57. The system of claim 56, further comprising:

server means for dynamically obtaining and sending authentication processes in response to client requests to take actions with respect to electronic documents; and

client means for interfacing with a received authentication process to identify a current user and for controlling actions with respect to electronic documents based on the current user and document-permissions information.